情報セキュリティ基本方針

インターネットの急速な普及、電子商取引の実用化など社会の情報化の進展に伴い、コミュニケーションの活性化への期待が高まり、情報化を取り巻く環境は急速に変化している。一方、情報化社会は多様な脅威に直面しており、さらにこの脅威は増加傾向にある。事業の継続発展のためにこのような環境変化と多様な脅威に的確に対応して行かなければならない。

株式会社小野運送店（以下、「当社」という。）が行う、一般貨物陸上運送、産業廃棄物処理業務、及び当社のすべての活動において、情報は他の重要な事業資産と同様に適切に保護する必要がある。事業損害を最小限にし、投資効率を上げた事業を維持・発展させ、広範囲にわたる脅威から情報を保護し、当社が提供するサービスの利用者や地域社会等からの期待と信頼に応えるため情報セキュリティ基本方針を定める。

1 目的

当社における全ての情報資産対する機密性、完全性および可用性を確保することを目的とする。
情報通信技術が急速に進展する中、情報資産に関する安全性の確保・リスク管理は不可欠な課題となっています。高度情報通信基盤を構築し維持管理することで、地域社会の発展と地域住民の生活向上に貢献を使命とする当社は、情報資産の安全性・信頼性を担保することが責務であることを改めて自覚し、情報資産に関して以下の通り総合的・継続的に取り組むための基本的な考え方、すなわち情報セキュリティ基本方針(以下「本方針」という)を示す。

2 用語の定義

情報システム	・ コンピュータ、ネットワーク及びそれらに付属するハードウェア/ソフトウェア等を含み構成された情報処理に用いる仕組みをいう。
電子情報	・ 情報システムにより通信および処理される電子的な情報 ・ 記憶媒体に保存された情報

印刷情報	・ 情報システムの開発と運用に関わる全ての文書 ・ 情報システムから出力・印刷された情報 ・ 契約書、見積書、注文書などの情報
情報資産	・ 組織が持つ「情報」と「情報システム」及び「これらが適切に保護され使用され機能するために必要な要件」の総称。 ・ 情報システム、電子情報、印刷情報、業務上知り得た情報・知識・ノウハウ
保有情報	・ 電子情報、印刷情報
記憶媒体	・ フレキシブルディスク、磁気テープ、磁気ディスク、光ディスク等電子情報を格納するもの
機密性（confidentiality）	・ 情報資産に対し正当な権限をもたないものがアクセスできないように保護し正当な権限をもつもの者であっても、その権限を越える内容で情報資産にアクセスできないように保護すること。
完全性（integrity）	・ 情報および処理方法の正確さおよび完全である状態を完全防護すること。
可用性（availability）	・ 情報資産に対し正当な権限をもつもの者が定められた方法に基づき何時でもアクセスできる状態。
情報セキュリティ	・ 情報資産の機密性、完全性および可用性が完全に確保し維持されること。
ネットワーク	・ コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）で構成され、情報処理を行う仕組みをいう。

3 適用範囲

3.1 場所の範囲

当社の敷地内、専用通信回線で結ばれた範囲、当社のケーブルテレビ・電気通信用伝送設備、その他当社の情報を取り扱うことを主たる目的とする物的設備の範囲とする。

3.2 人的範囲

(1)当社の取締役、監査役等の役員、従業員、派遣社員、臨時雇用者（アルバイト、パート）等、当社と雇用契約関係を持つ者(以下「当社従業員」という)を対象とする。
(2)当社が外部事業者等との間で業務委託契約などを締結し、当社の保有情報を使用した業

務を行わせる場合、別途定める「業務委託契約書」に本方針を遵守することを明記し契約を取り交わす。
(3) 雇用契約関係及び業務契約関係が終了した者においても、「秘密保持に関する誓約書」をその者との間で取り交わすなどして本方針の対象とする。

3.3 時間的範囲

当社に入社ないし各種契約が成立したと同時に適用となり、退社後も保有情報に関する限り適用されるものとする。雇用契約関係及び業務契約関係が終了した者においても、「秘密保持に関する誓約書」をその者との間で取り交わすなどして本方針の対象とする。

4 セキュリティ組織（運営体制）

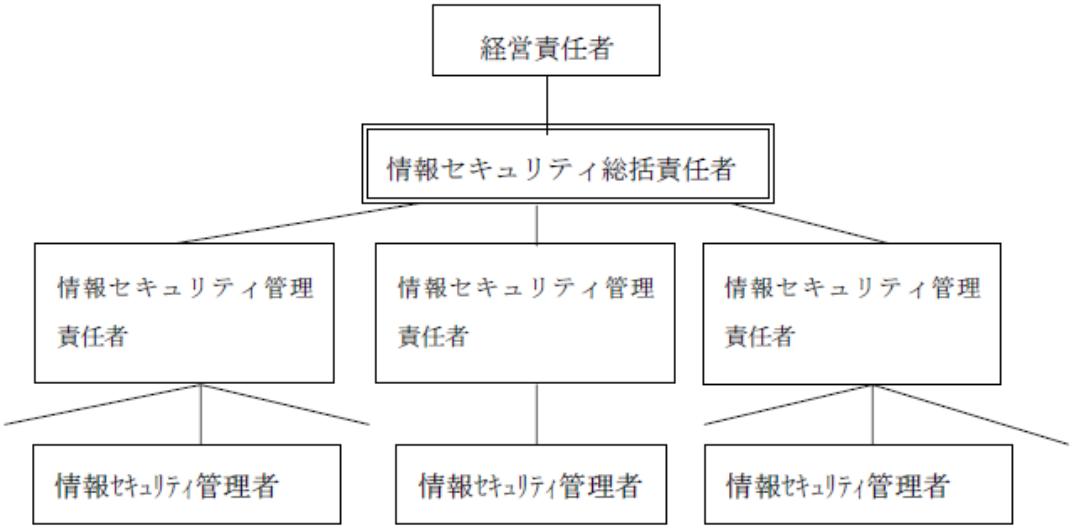
4.1 運営委員会

適切な責任及び資源の配分によって当社内における情報セキュリティを促進するため、情報セキュリティ運営委員会（以下「運営委員会」という。）を設置し、運営委員会は主に次のことを行う。
(1) 本方針並びに全体的な責任の見直し及び承認。
(2) 情報資産が重大な脅威にさらされていることを示す変化の監視。
(3) 情報セキュリティの事件・事故の見直し及び監視。
(4) 情報セキュリティを強化するための主要な発議の承認。
(5) 情報セキュリティのための個別の基準・規則・手順書の同意及び支持。
(6) 本方針の遵守の励行および違反に対する措置。

4.2 運営委員会の組織と責任

運営委員会の組織と責任を次のように定める。
・経営責任者（全ての情報資産の情報セキュリティを統括する最高情報統括責任者）
・情報セキュリティ統括責任者
・情報セキュリティ管理責任者（各部門長）
・情報セキュリティ管理者
・情報セキュリティ管理者

・システム管理者並びに運用責任者



5 法令の遵守（コンプライアンス）

情報資産に対する各種脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講じるものとする。

主な情報セキュリティ関係法令

*1 個人情報の保護に関する法律 http://www.kantei.go.jp/jp/it/index.html

*2 不正アクセス行為の禁止等に関する法律

*3 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律 http://www.soumu.go.jp/joho_tsusin/top/denki_h.html

*4 特定電子メールの送信の適正化等に関する法律

*6 電子署名及び認証業務に関する法律

*7 著作権法

*8 不正競争防止法

*9 犯罪捜査のための通信傍受に関する法律

*10 刑法

*11 行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律

*12 行政機関の保有する情報の公開に関する法律

6 情報セキュリティ対策

情報資産に対する各種脅威（ウイルスや悪意あるソフトウェアなど）から情報資産を保護するために、次に掲げる情報セキュリティ対策を実施するものとする。

6.1 保有情報の分類と管理

情報資産の重要度を判断する基準を明確化し、その重要度に応じ情報システムの利用者が適正に情報システムを運用するため、情報資産分類と管理方法の対策を講じる。これにより権限を持たない者による不正な情報システムの運用やアクセスを防止する

6.2 物理的セキュリティ対策

情報システムを設置する施設への不正な立入りおよび情報資産への損傷、妨害等から保護するために物理的な対策を講じる。

6.3 人的セキュリティ対策

情報セキュリティに関する各責任者、運用者、利用者等の権限と責任を定め、当社従業員に本方針および関係法令の内容を周知徹底する等、十分な教育および啓発が行われるよう必要な対策を講じる。
また、業務委託するに当たり、委託業者による不正な情報資産の取り扱いを防止するための対策を講じる。

6.4 運用におけるセキュリティ対策

緊急時に迅速かつ適切な対応を可能とするための危機管理および情報セキュリティ対策の遵守状況を確認するための運用面の対策を講じる。

6.5 ウイルス及び悪意あるソフトウェアの予防及び検出

情報システムに対するウイルスや悪意あるソフトウェアなどの侵入を防止し、検出するため情報システムに予防の処置を講じることとし、さらに利用者には危険を知らせることを行 う。

7 本方針に対する違反の措置

(1) 従業員は、セキュリティを確保するため関係法律や本方針、及び本方針の個別方針や基準・規則を遵守しなければならない。これらに対する違反の行為を行った者は、当社就業規則に従い処置することとする。

(2) 当社と業務委託契約関係にある外部事業者においても、関係法令や本方針を遵守することとし、これらに違反があった場合には業務委託契約等に基づき処置することとする。

8 情報セキュリティの事件・事故の報告義務

情報システムに携わるすべての者は、情報セキュリティの事件・事故があった場合には別に定める連絡体制に従い遅滞なく連絡することとする。
報告を受けた各責任者及び管理者は事業継続管理基準に従い必要な処置を行うこととする。

策基準の策定

9 対策基準の策定

６項に示す対策を講じるにあたり、遵守すべき行為および判断などの統一的な基準を規定などで定めるために必要となる基本的な用件を明記した対策基準を策定する。

9.1 規定等の整備

情報セキュリティを講じるにあたり関係部門は、本方針および対策基準により情報セキュリティに必要となる基本的な要件を明記した規定などを整備する。

10 **の策定** 実施手順書（運用マニュアル）

本方針の具体的な実施手順は、全社的に定めることが望ましいが、組織の規模・構成・運用を鑑み、部毎に定めてもよい。
対策基準に基づき整備された規定などを遵守して情報セキュリティ対策を実施するため、各情報システムの主管部門は、主管する情報システムについて具体的な実施手順を明記した「情報セキュリティ実施手順書」を策定する。
なお、情報セキュリティ実施手順は、公開することにより会社の事業活動、運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

11 当社従業員と外部事業者の情報セキュリティの教育

情報セキュリティ統括責任者は、本方針および対策基準・規定・運用手順書が適正に実施されるよう、当社従業員と外部事業者へ関係法令・本方針および関係基準・ガイドライン等について啓発、意識向上のため、教育プログラムを策定し実施する。

12 監査

当社は、情報セキュリティ監査委員会を設置し、情報セキュリティ対策の遵守状況および実効性の有無などを検証するため、定期的（毎年６月）に監査を実施する。
情報セキュリティ監査委員会は、代表取締役社長が設置し、監査委員を指名する。

13 評価および見直し

運営委員会は、情報セキュリティの監査結果などにより本方針に定める事項及び情報セキュリティ対策の実効性を評価するとともに、情報システムの変更、情報セキュリティを取り巻く状況の変化に対応するため適宜本方針の見直しを実施する。

- **セキュリティの事件、事故を記録保存し、回数や影響度によって示される本方針の有効性**
- **情報セキュリティ管理策の費用を含む事業効率**
- **設備の変更、技術変更や組織基盤等の変更に伴って及ぶ影響**

以上、本方針を支持し、これを全従業員に対して公表し、本方針を運用する。
令和５年９月３０日

東京都品川区南品川四丁目２番３３号
株式会社　小野運送店
代表取締役社長小野　正彦　　印

経営責任者の情報セキュリティ確保の宣言文

当社は、『地域社会の発展と、地域住民の生活向上に貢献することを使命』とし、かつ、『総合顧客満足度を向上させること』を品質目標に掲げ、物流・産業廃棄物処理といった総合的な地域サービスを提供することを企業理念としている。私たちは、この企業理念に基づき、地域社会および顧客からの信頼と期待に応えるべく、お預かりした、あるいは知り得た情報をはじめとして、当社が取り扱う全ての情報資産を多様な脅威から守るため、また、健全な管理を徹底するため、その取り扱いに関する『情報セキュリティ方針』を定め、これを当社役員、社員、更には協力会社関係者および委託先を含め、周知させ、もって総合顧客満足の向上と社会への貢献に鋭意努める。

令和５年９月３０日

株式会社 小野運送店

代表取締役社長小野　正彦